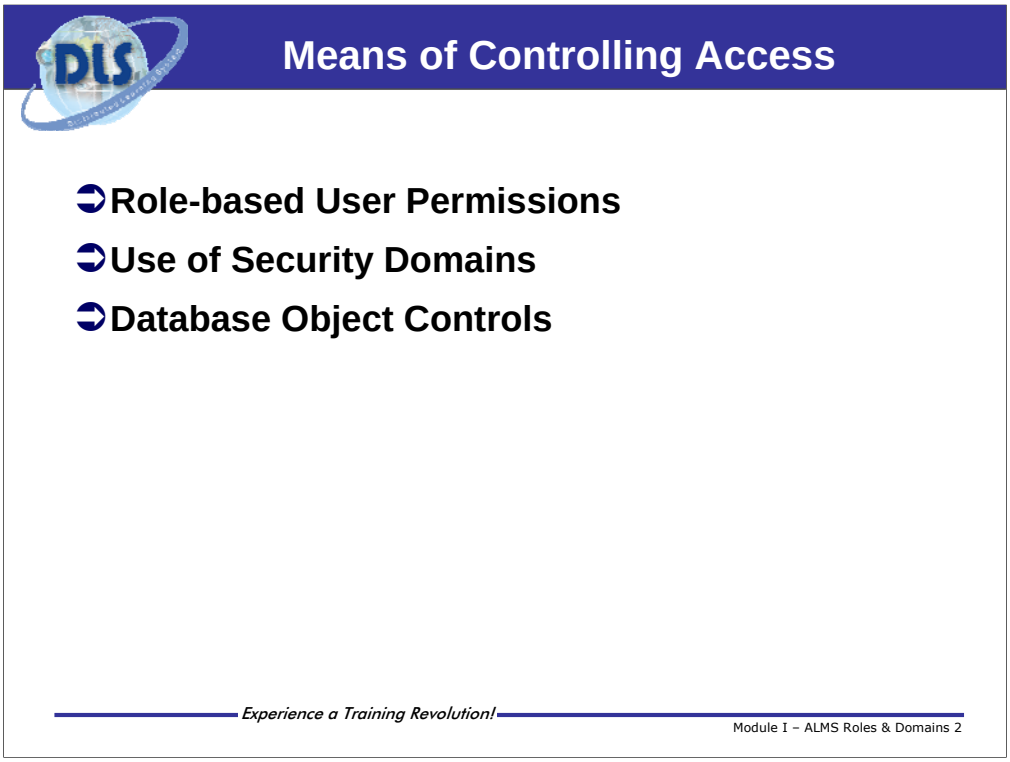

PEO EIS
DLS
Distributed Learning System
ALMS Roles & Domains
Office of the Project Manager, Distributed Learning System
Experience a Training Revolution!

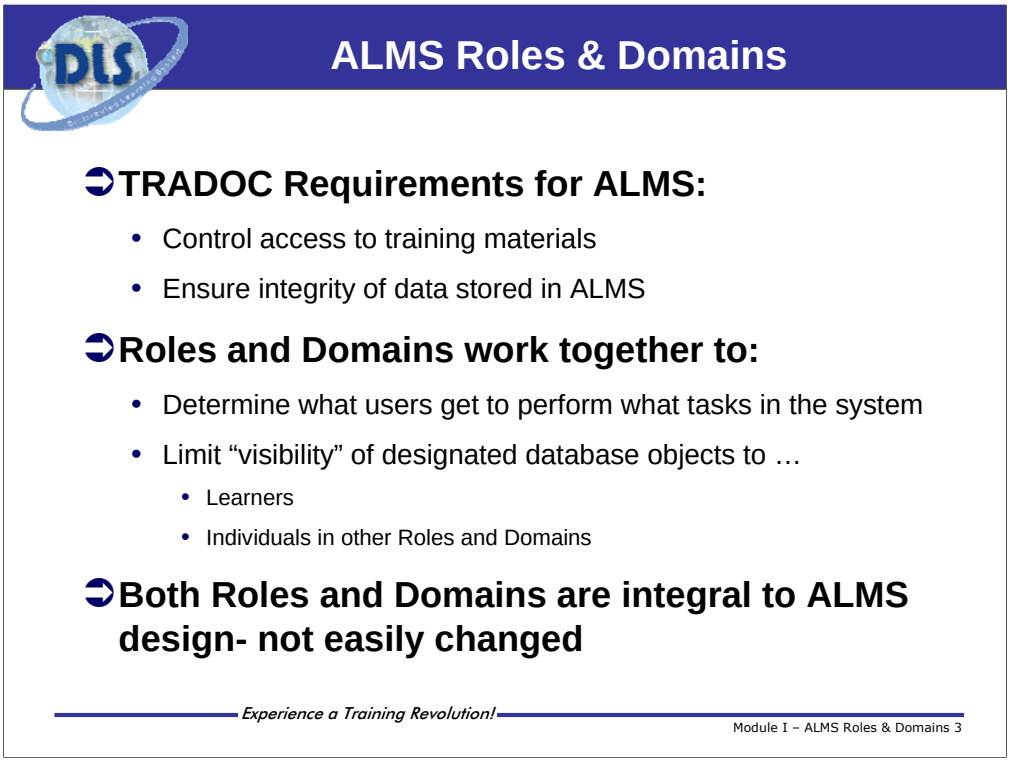


The ALMS employs three major methods for controlling access to data. The control of access in the LMS is how training is made available to Learners or not, and ensures the integrity of data objects stored in the DB.

1st Bullet: User Roles enable and restrict the functions individuals in those Roles perform in the system. Simply, the Role a user has been assigned in the system control his access to data and therefore the functions he or she can perform.

2nd Bullet: Most major data objects have domains associated with them. An object's Domain determines who have privileges to read, write, copy that object. In practical terms, the Domains of training data objects such as Courses, Resources, and, even people, will determine how they behave and what they can do in the LMS training environment.

3rd bullet: Besides Roles and Domains, there are several built-in features that users can employ to control access to various database objects. We'll look at these briefly a little later…



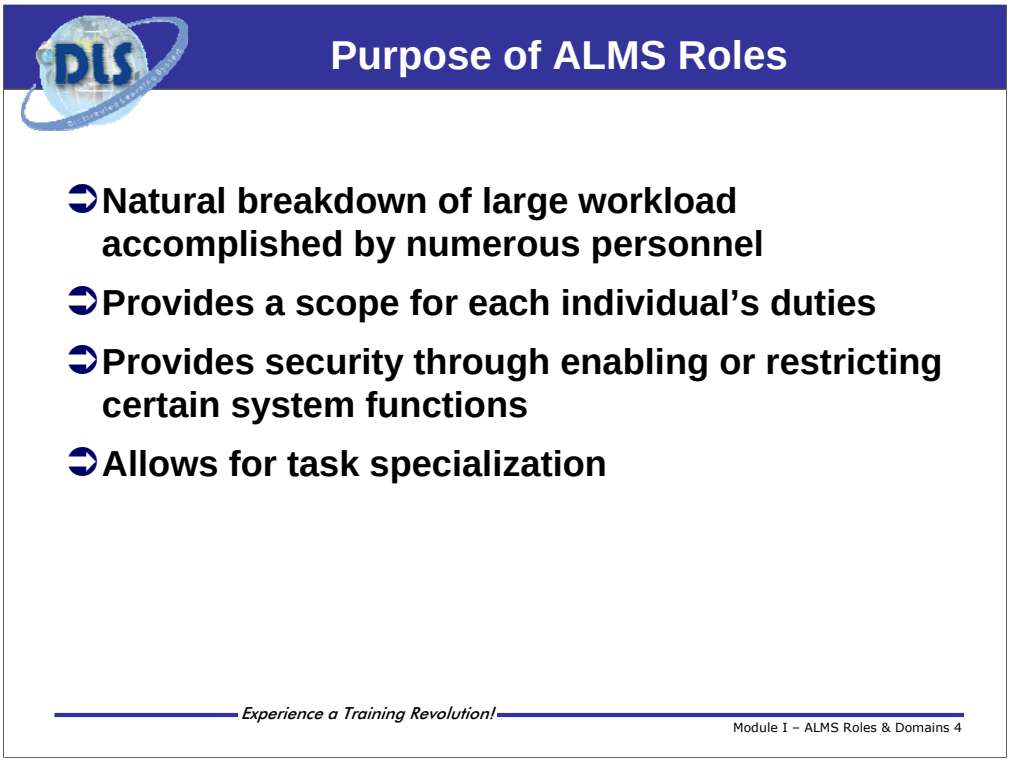
We train Roles and Domains early in ALMS training because they are fundamental to how the system operates.

1st Bullet: When the ALMS contract requirements were put to bid, two sets of requirements were included that resulted directly in the LMS implementation of Roles and Domains: controlling access and data integrity.

2nd bullet: ALMS Roles and Domains fulfill those requirements. They are closely linked and are used in combination, and with other system features, to determine system privileges. They control the ability of users to read, write, and copy database objects. These privileges and restrictions apply both to Learners and other Role Based Users.

3rd Bullet: Roles and Domains are deeply woven into the system design and database architecture. They can be changed, but not easily or cheaply.

Let's look at Roles first…

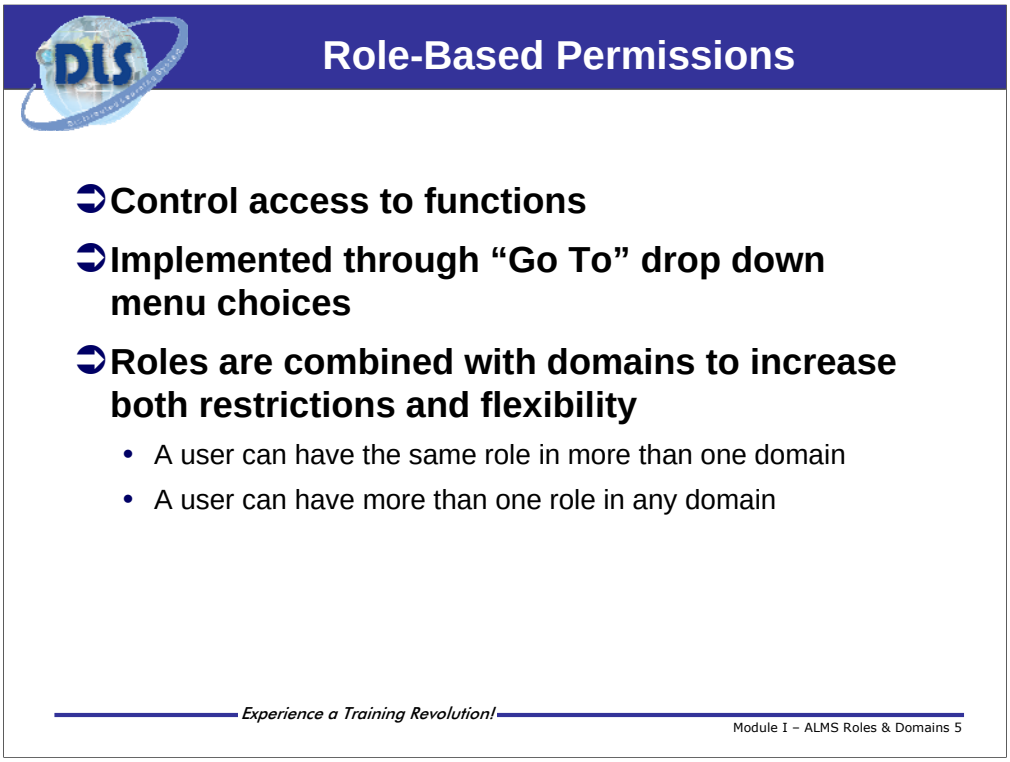


1st Bullet: In any complicated process that involves the coordinated actions of several individuals, it is natural for those individuals to specialize to some degree. People find niches and work in them, each contributing some small part to the whole. ALMS Roles simply formalize that natural tendency.

2nd Bullet: By formalizing the specialization tendency into Roles, each individual in the process has a specific set of tasks that correspond to his Role. These are the *permissions* granted by the system for that Role.

3rd Bullet: Restrictions are the opposite of permissions. The ALMS enforcement of restrictions provides security for data stored in the system and ensure everyone involved in the process "stays in their lane."

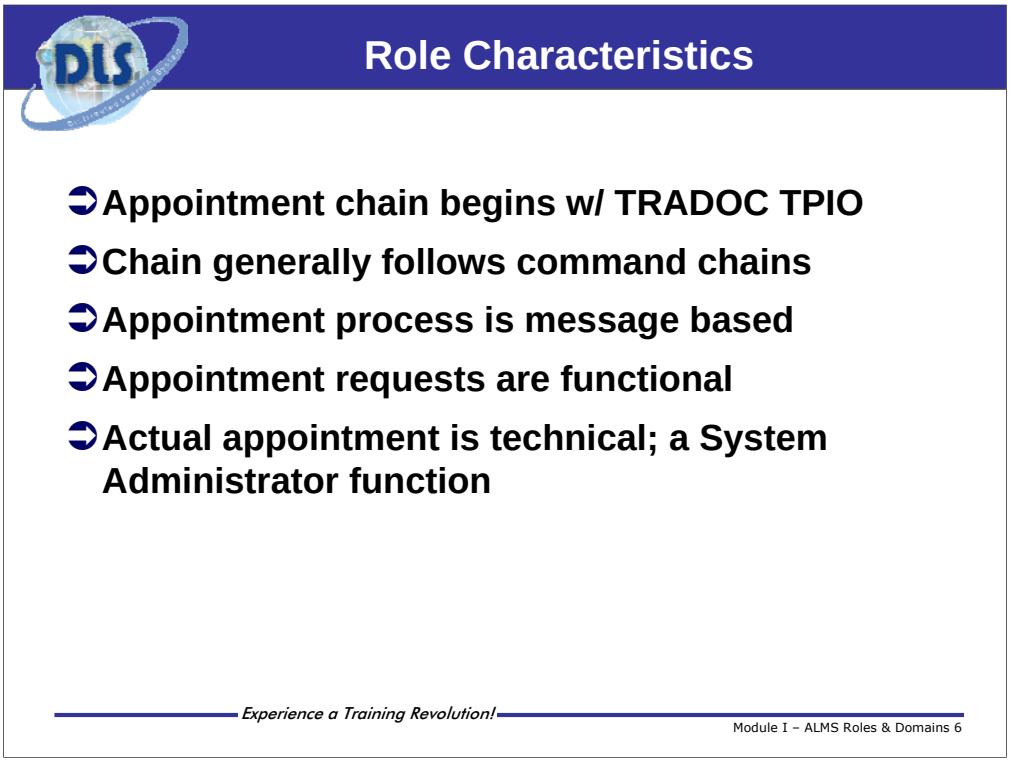
4th Bullet: The task specialization enforced through the use of Roles enables individuals to acquire areas of expertise. The appointment of additional Roles permits that person to broaden his training support task proficiency.



1st Bullet: The use of Roles controls access to functions, things you can do in the system, by enforcing task specialization.

2nd Bullet: The ALMS implements the use of Roles through the Go To drop-down menu, available from most screen in the system. Your Role control what choices you can make from the menu and also controls the actions you can perform after using the Go To menu to navigate through the system.

3rd Bullet: We've said that Roles and Domains work together. A user's permissions are governed by both when attempting to perform ALMS functions. Yet, they can also be combined in multiple ways to increase the flexibility the system has in matching its functions to organizational business processes.



This slide shows some of the features or characteristics concerning ALMS Roles…

1st Bullet: Because Role Based Users in the ALMS have access to individual's personal data, can post information to official training records, and manage test questions and answers, it is important to establish and maintain a chain of appointments. This ensure that there is a responsible official on record for every appointed Role Based User. The sequence begins with the TRADOC Program Integration Officer, at TRADOC Deputy Chief of Staff for Operations &Training.

2nd Bullet: Whenever possible, the ALMS appointment will use the chain of command already established in the Army.

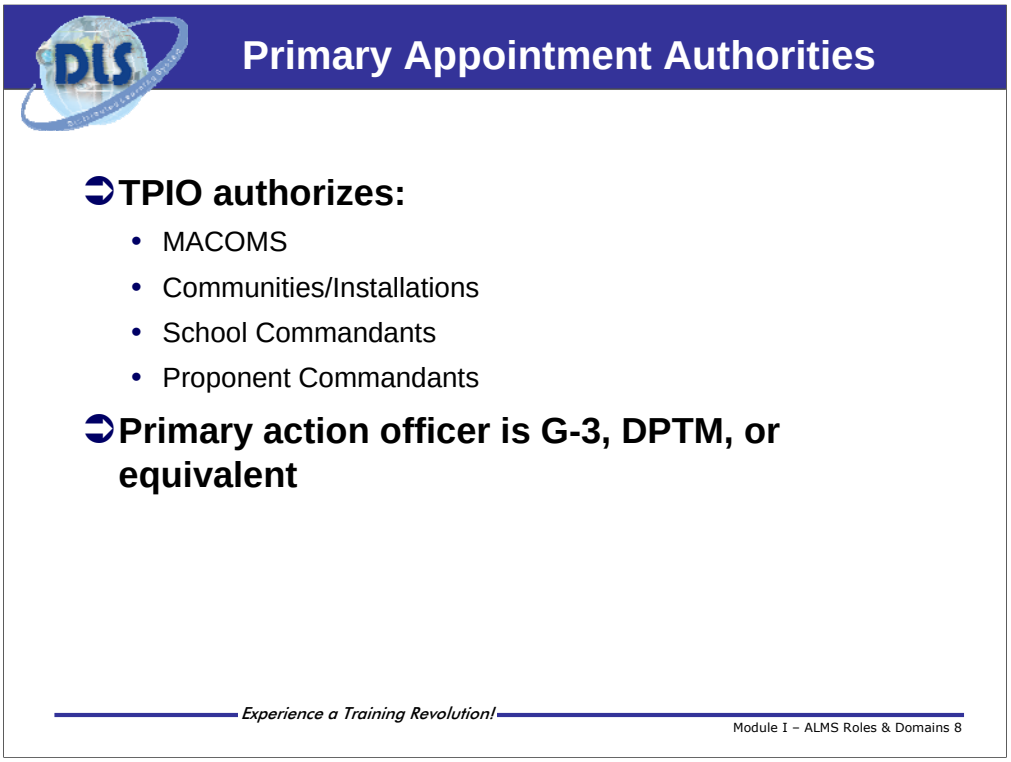
3rd Bullet: It is necessary that there be a written trail for appointments. So, the ALMS will utilize the Army Training Help Desk (ATHD) message forms- the same process for making any administrative requests of the ALMS and for asking questions.

4th and 5th Bullets: The ALMS ATHD personnel rely on the training community as the functional representatives in determining what permission are granted to each Role Based User. The System Administrators perform the technical work to enable the request.

Available Roles in ALMS

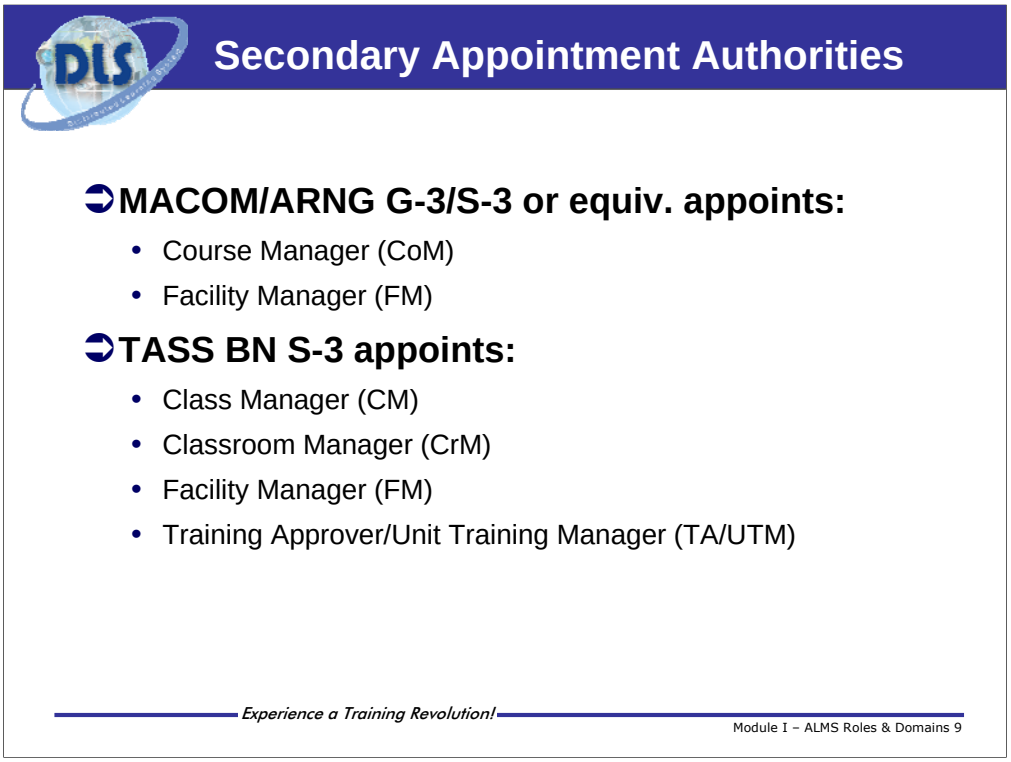
The following ALMS roles provide the human interface with the ALMS; Role Based Users (RBU) are the Data Owners needed for system functionality:

- **Faculty Roles**
  - Instructor
  - Assistant Instructor
  - Subject Matter Expert
  - Facilitator
- **Scheduler**
- **Class Manager**
- **Course Manager**
- **Learner**
- **Resource Mgr Roles**
  - Classroom Manager
  - Facility Manager
  - DTF Manager
  - Product Distributor
- **Unit Roles**
  - Training Approver
  - Unit Training Manager
- **System Administrator (at EMC)**

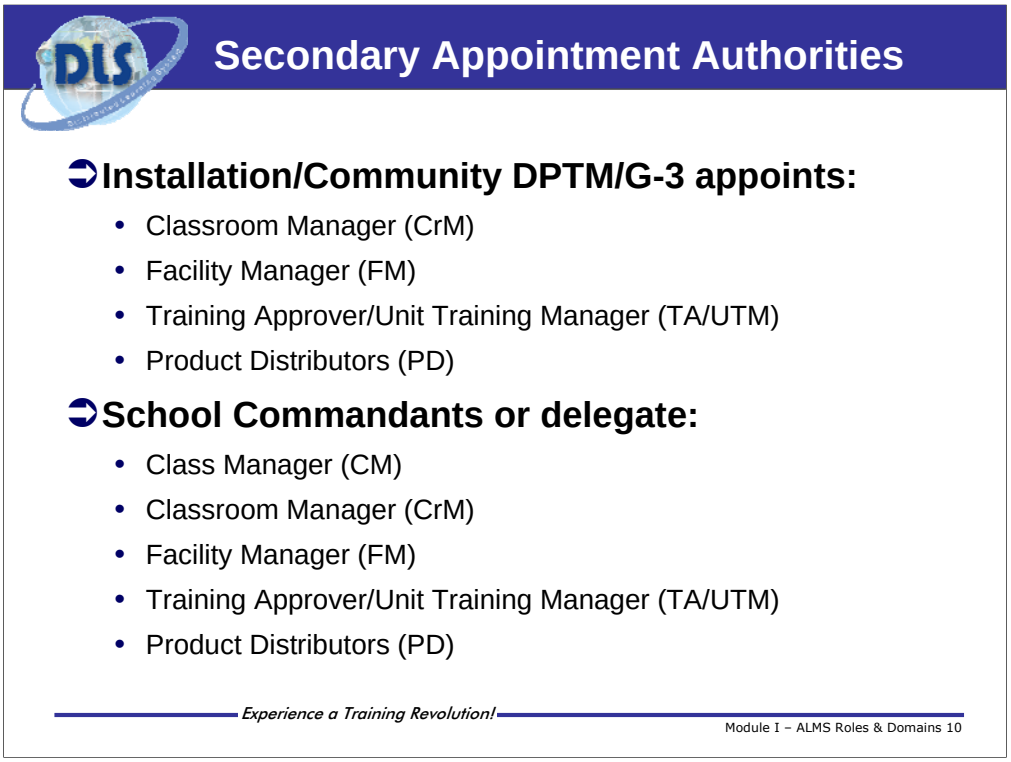


The next few slides show how the ALMS Role Based User authorization chain works. We won't spend time detailing the positions and their authorizations. Details can be found in the Training SOP.

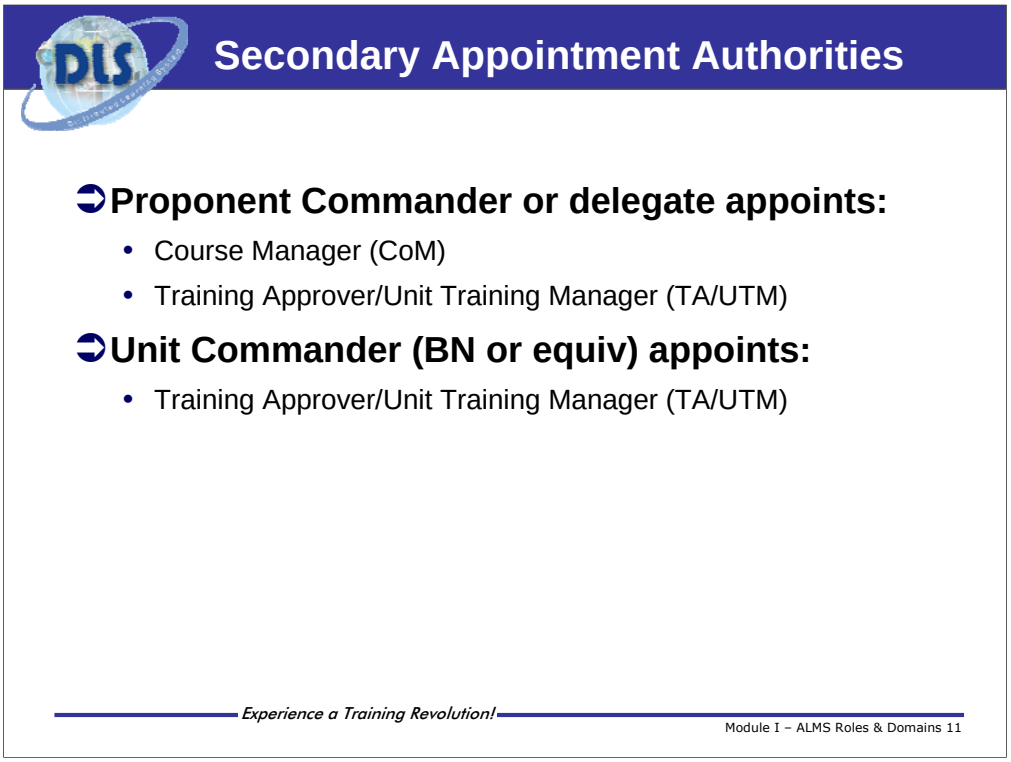
The chain begins with the TPIO. He makes these appointments.



MACOM and TASS BN representatives can make these appointments…

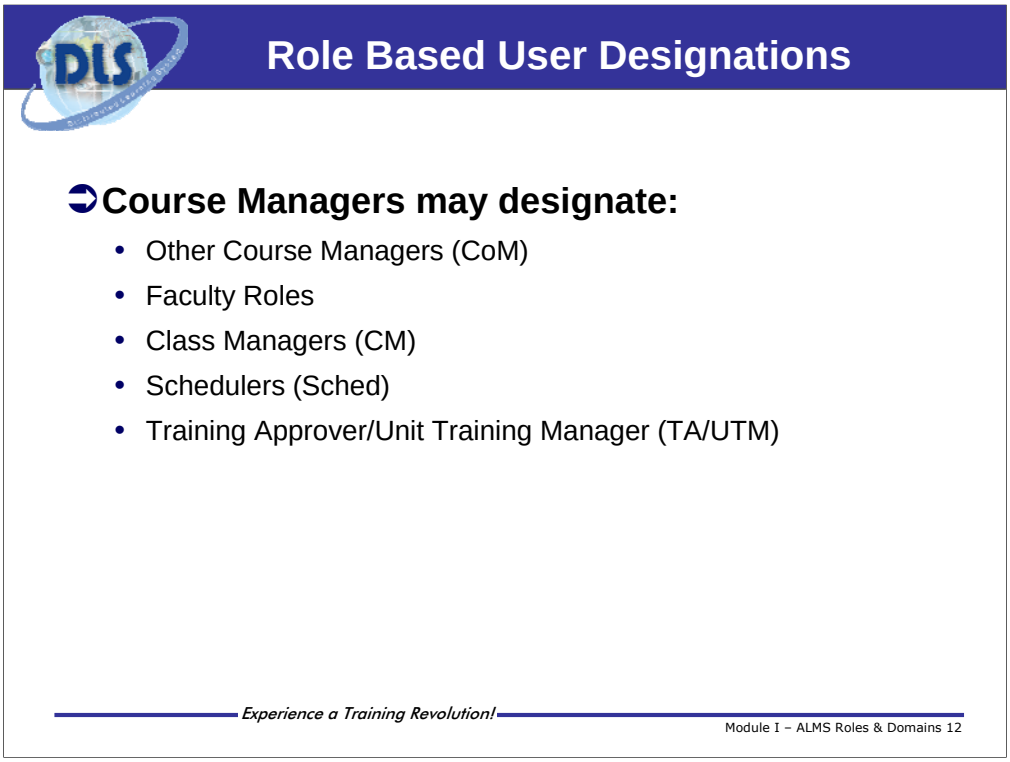


These sets of appointments center mainly around organizations that execute training, rather than function as the Proponents of training material…

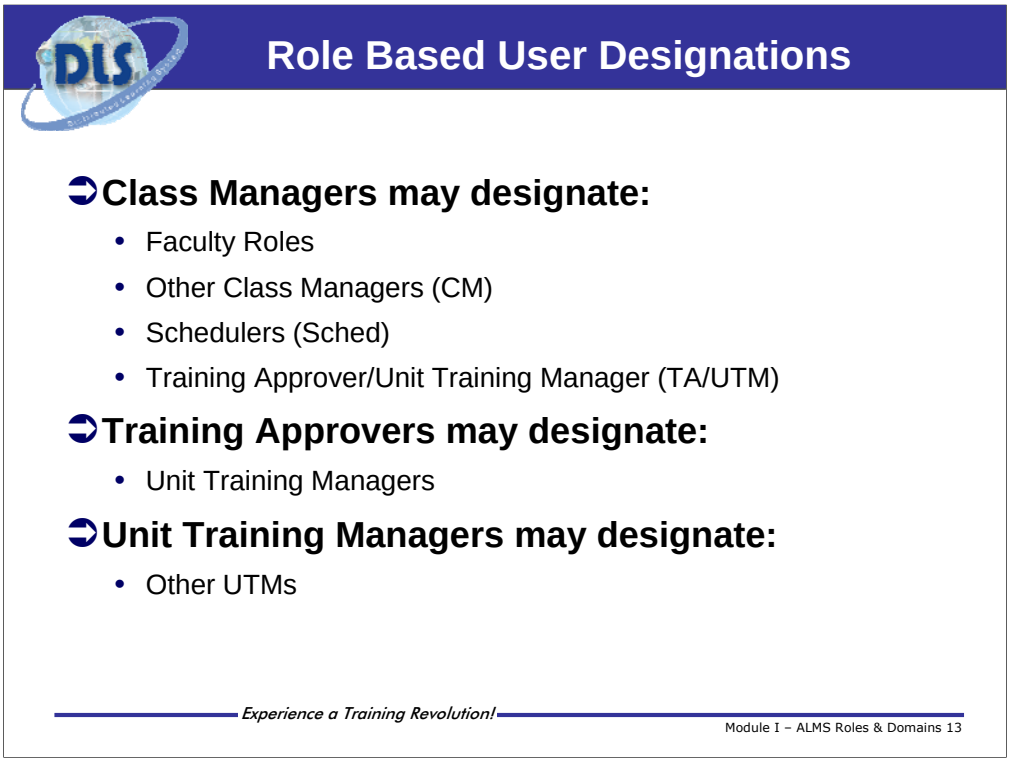


Often the Proponent organization also functions as a training institution such as with TRADOC. For a TRADOC installation, these appointments are couple with those for a School.

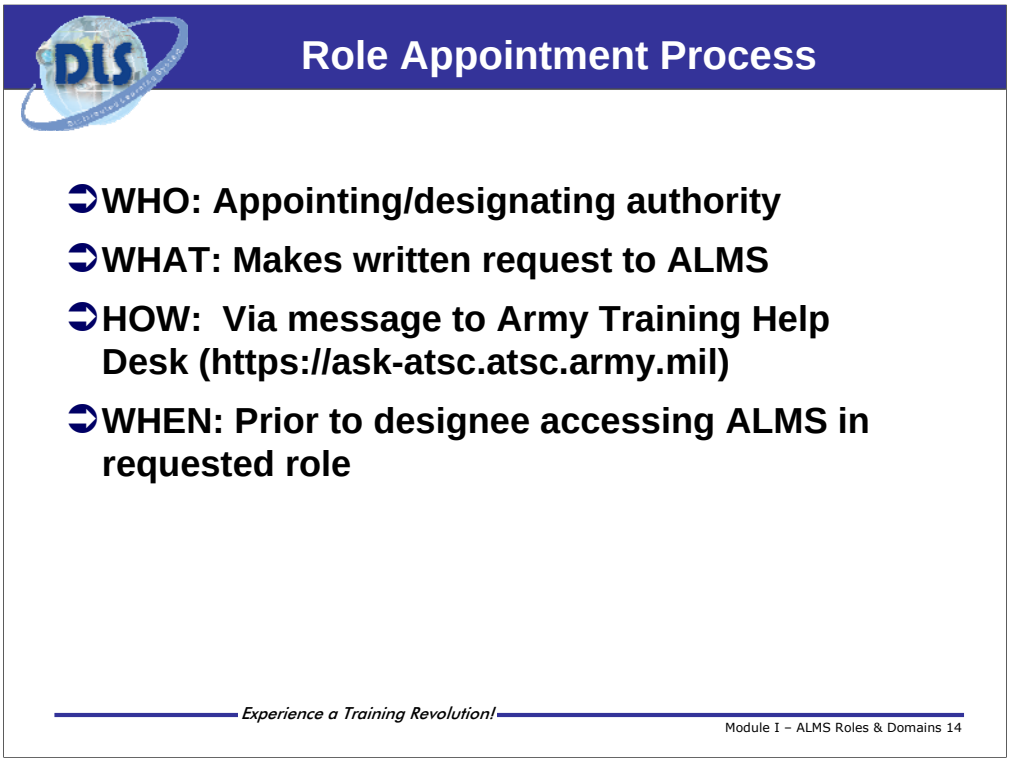
Units only need appoint Learning Approvers and training managers.



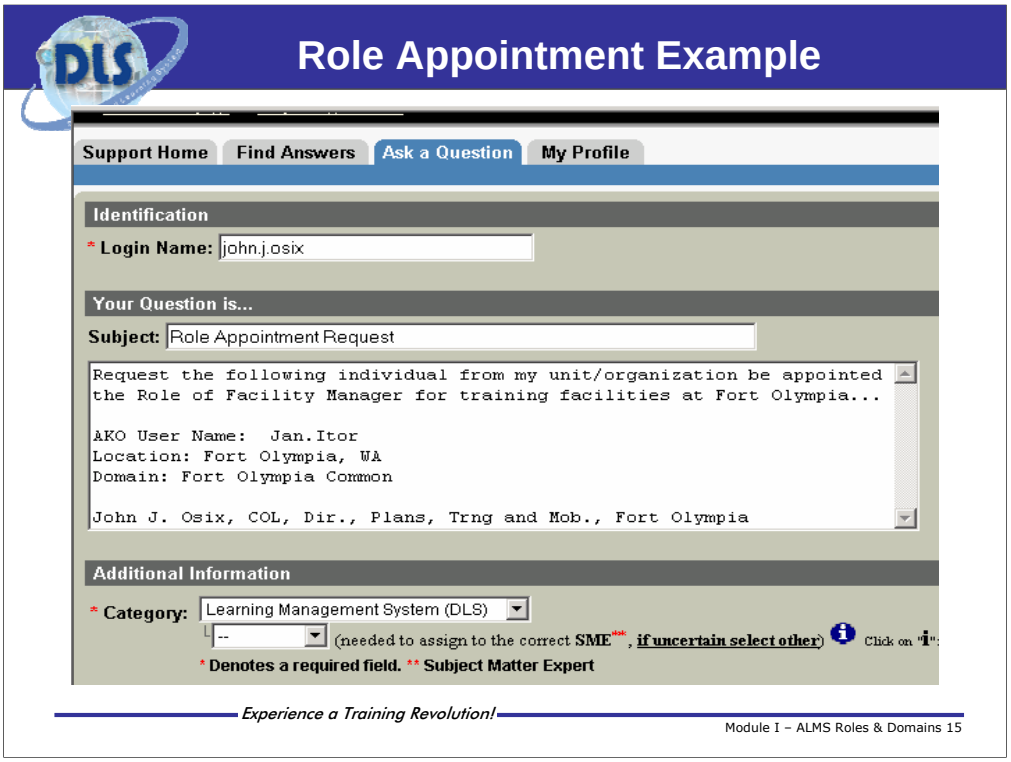
To streamline the process, some RBUs are permitted to make appointments of other RBUs. We call these designations. The process is the same– a message to the ATHD.



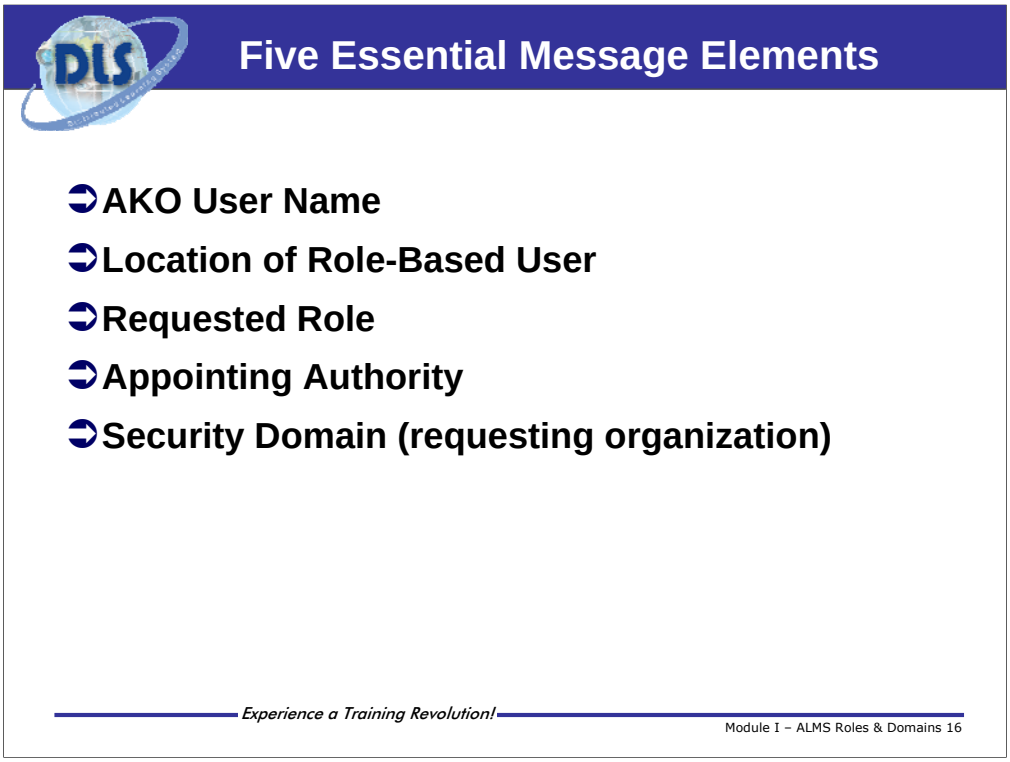
Here are other designations that RBUs can make …



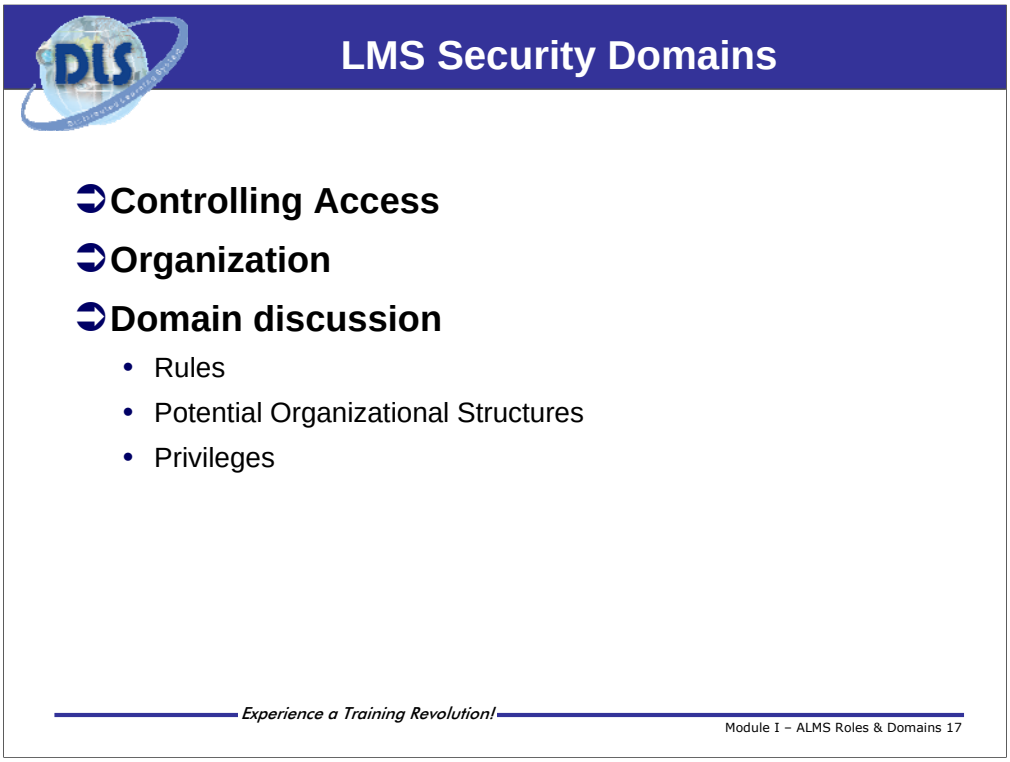
Here is the procedure for making a request for the appointment or designation of a RBU. Note that the use of the ATHD at "ASK-ATSC" is **not email**. Once at the URL above, there is a free text message capability contained at the site.



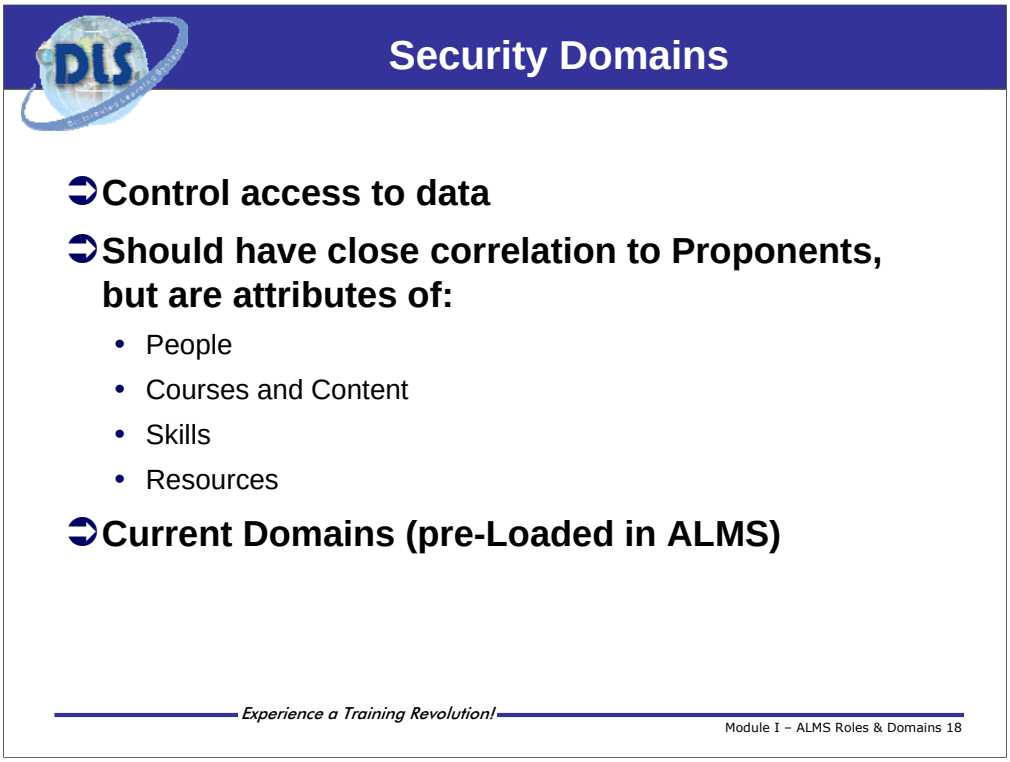
Here is what an appointment request message looks like in ASK-ATSC. Note that certain relevant pieces of information are present. These are the essential elements for a request…



Those essential elements are…



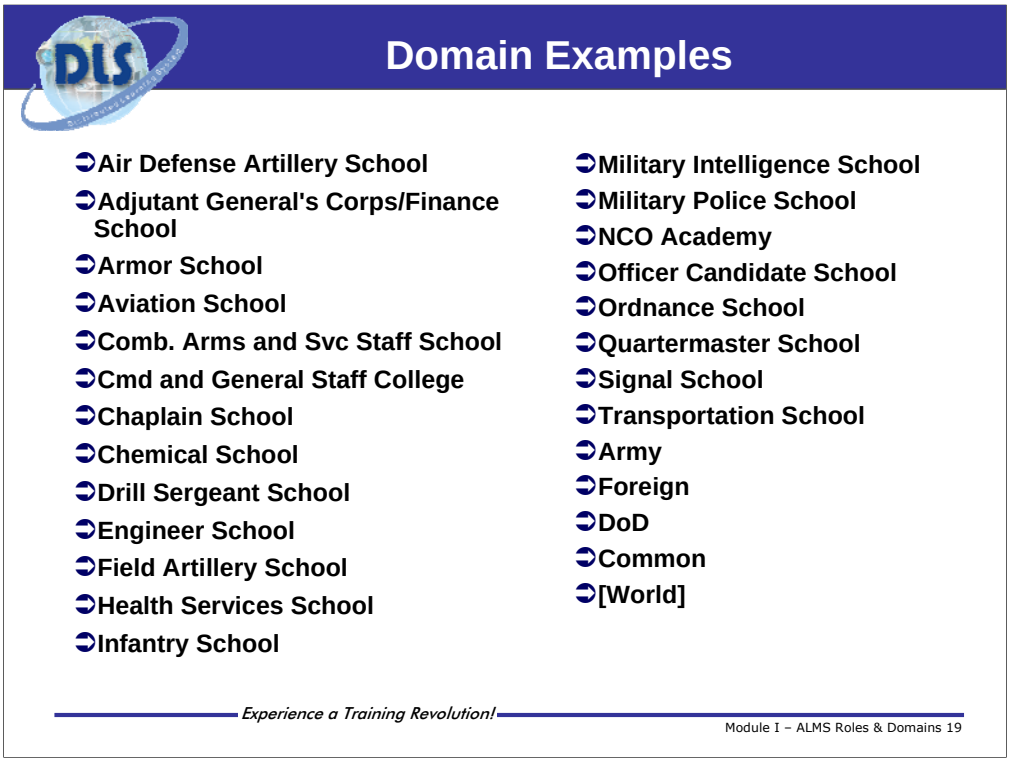
Moving from the discussion of Roles to Domains, we will discuss how they are used to control access to data in the ALMS, how they are organized, and we will discuss rules for employing Domains, how they might fit different organizations, and what privileges and restrictions are associated with Domain use for various data types and user Roles.



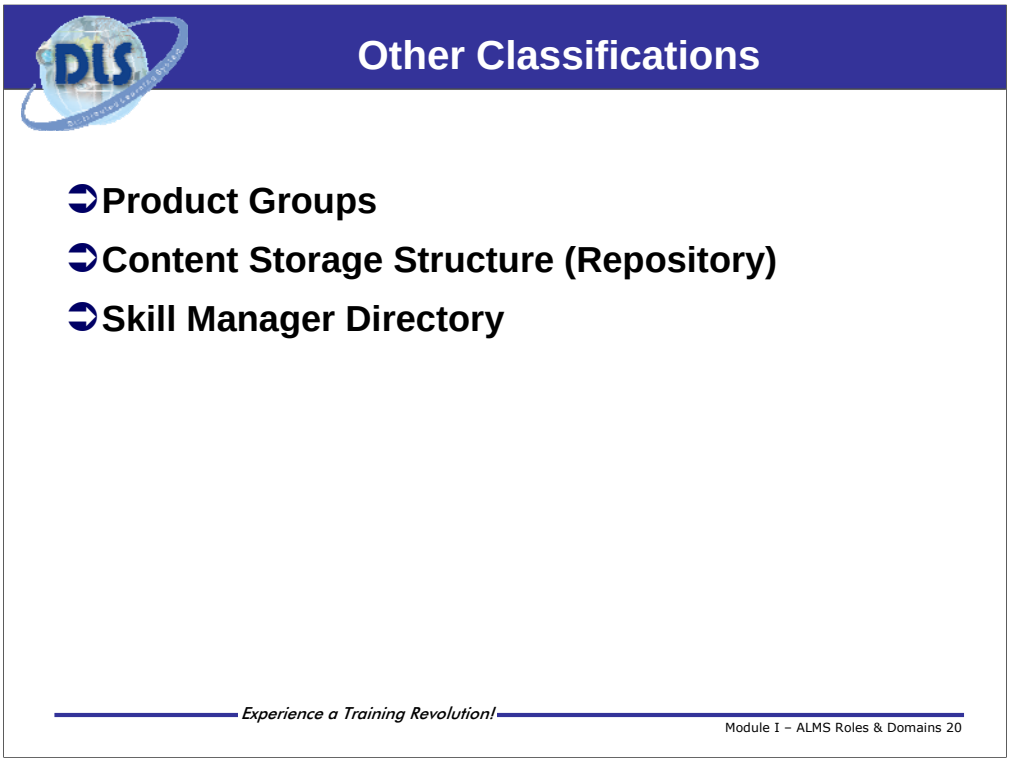
1st Bullet: Like Roles, Domains control access to data in the system. That control has direct impact on how the data behaves and can be used to support organizational business processes when implemented.

2nd Bullet: Most of the Domains pre-established in the ALMS have a close correlation to functional Proponent agencies. That is because training material always has a Proponent or owner responsible for its content. Domains, however, are required for other major data objects, and can be used to control the accessibility of these objects in the system.

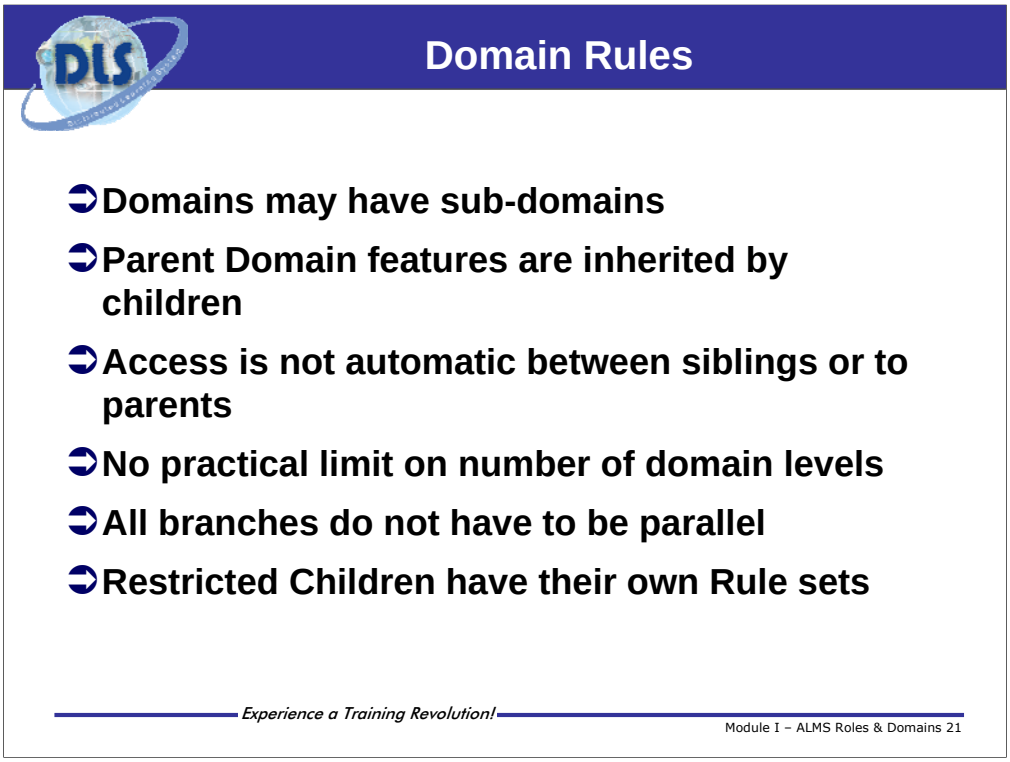
3rd Bullet: As indicated, there is a list of Domains which come pre-populated in the system. They are:



As you can see, there is definitely a Proponent flavor to this list. Because the ALMS is being fielded to TRADOC first, this list should suffice for the first year at least. Note that adding, deleting, or changing entries on this list is difficult and expensive. We will be happy to work with data owners of all types to ensure that their data functions according to their needs to the greatest extent possible.



The ALMS has other means of classifying data groups that may look like the Domain structure. Product, content, and Skills data groups all have these attributes. However, these classifications are intended to be useful for organizing, sorting, searching, and filtering data. They don't control system functions or access.



Here is some basic rules for employing Domains with data groups. Understanding the rules will aid in making decisions about what Domains to place data objects in. Each Domain may be further divided into sub-Domains. We sometimes call them Parent and Child Domains. When used, they occupy two Domain levels, the Parent level above the Child. Two sub-Domains or Children from the same Parent are Siblings and occupy the same Domain level.

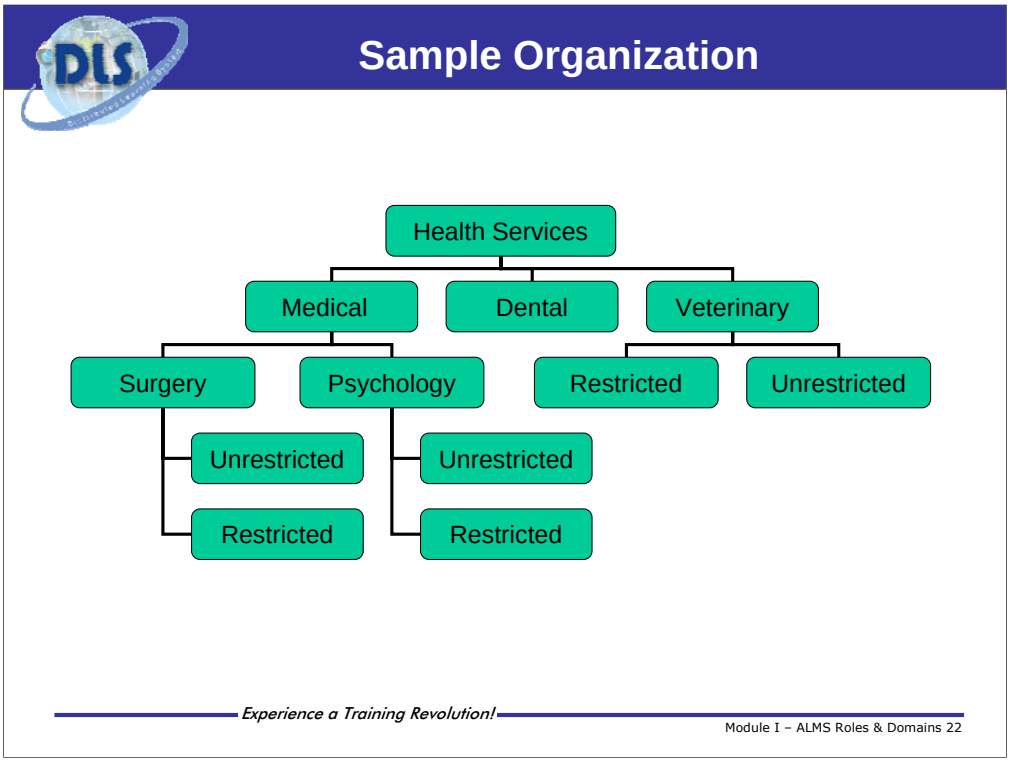
1st Bullet: A common example of a sub-Domain is the restricted portion of any existing Domain, such as Artillery Restricted.

2nd Bullet: Children sub-Domains will carry the characteristics of their Parent. Members of the Parent Domain may access objects placed in their sub-Domains.

3rd Bullet: Generally, two Children of the same Parent or Siblings cannot have full access objects in each other's Domains nor have full access objects in the Parent Domain.

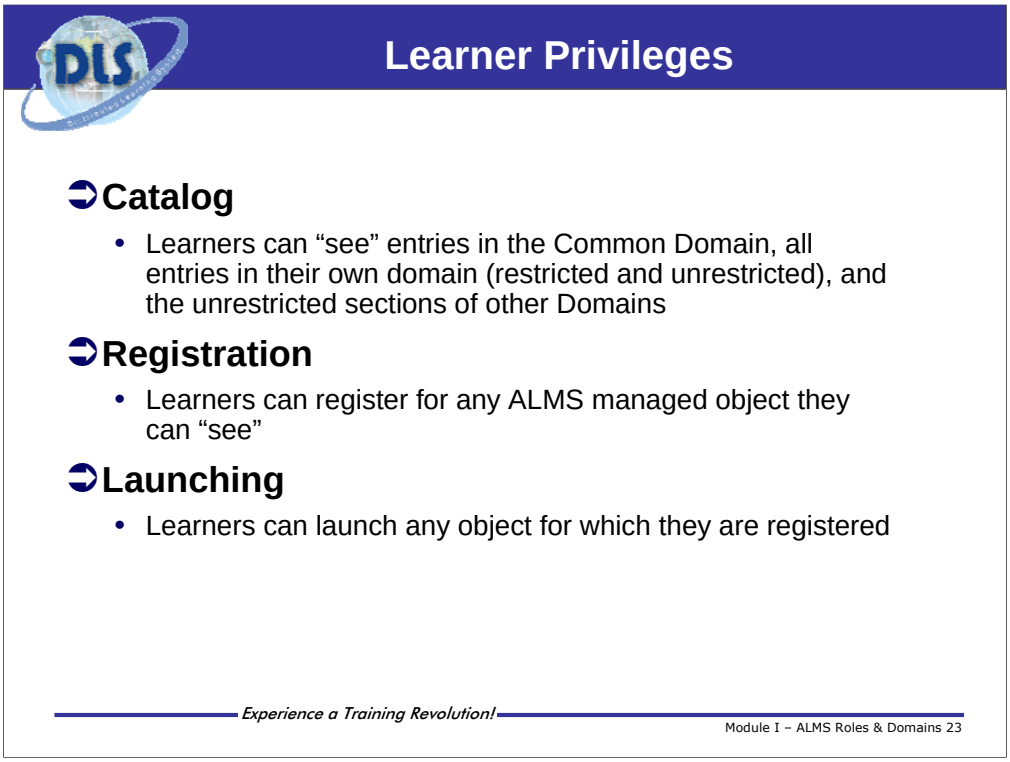
4th Bullet: The technical limit on Domain levels is so large as to be practically unlimited. However, organizations will see how the creation and management of numerous sub-Domains and Domain levels is likely to be more trouble than it is worth.

5th Bullet: This just means that if one Child Domain has its own Child, its Siblings don't necessarily have to have Children.



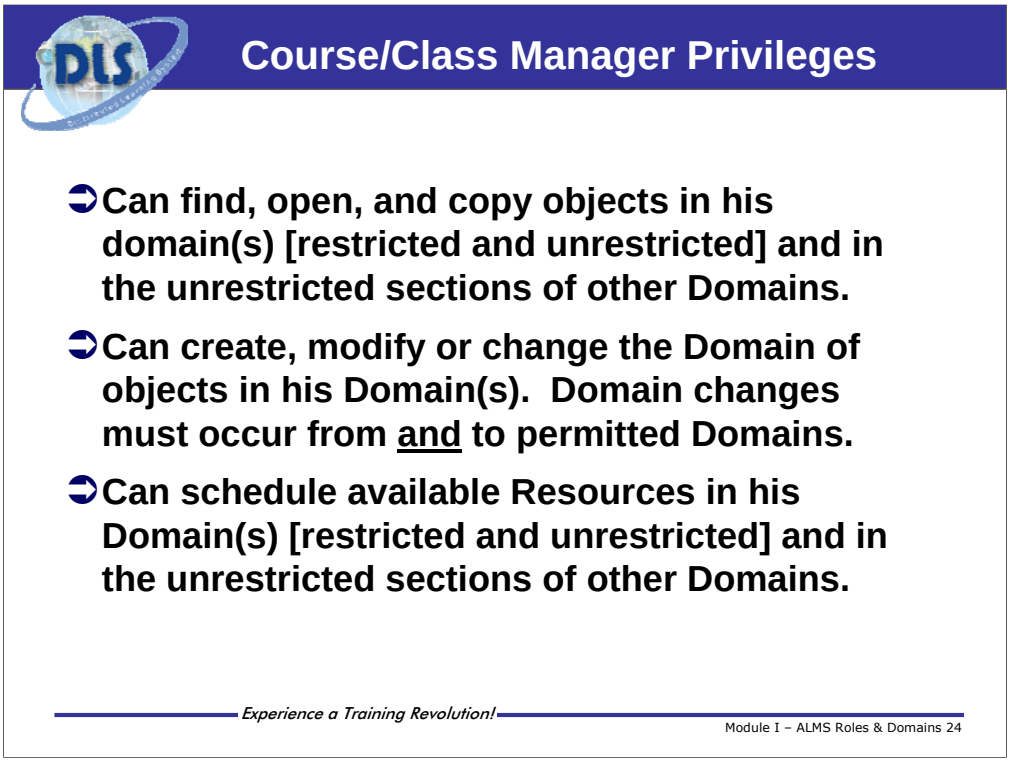
Here is an example of how one organization, Health Services, might employ Domains. Note that there are three sub-Domains or Children of the Parent. The Medical Child has Children sub-Domains (Surgery and Psychology), each with Restricted and Unrestricted portions. Dental has no Children. Veterinary has only the Restricted and Unrestricted sub-Domains.

An organization whose Domain structure is this detailed may prove to be too complex for many Branches.

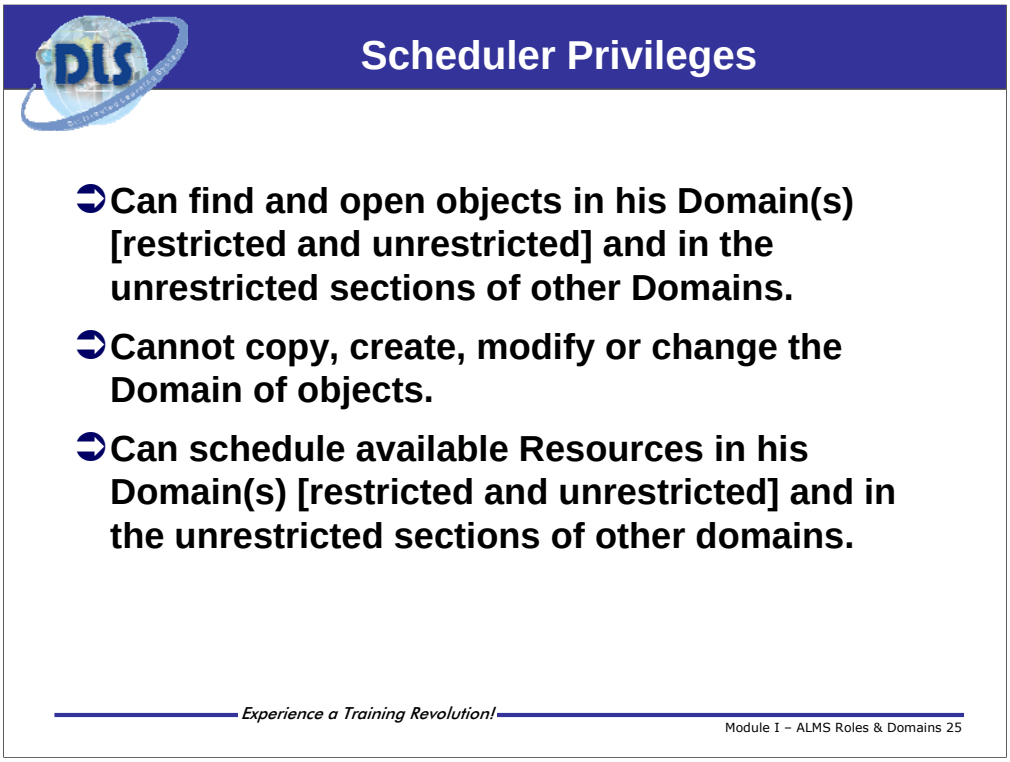


Here is how Domains work for Learners… [Trainer read bullets]

What these mean taken together is that a Leaner in the Transportation Domain can, for example look up, register for, and run Courseware that is in the Unrestricted Quartermaster Domain.



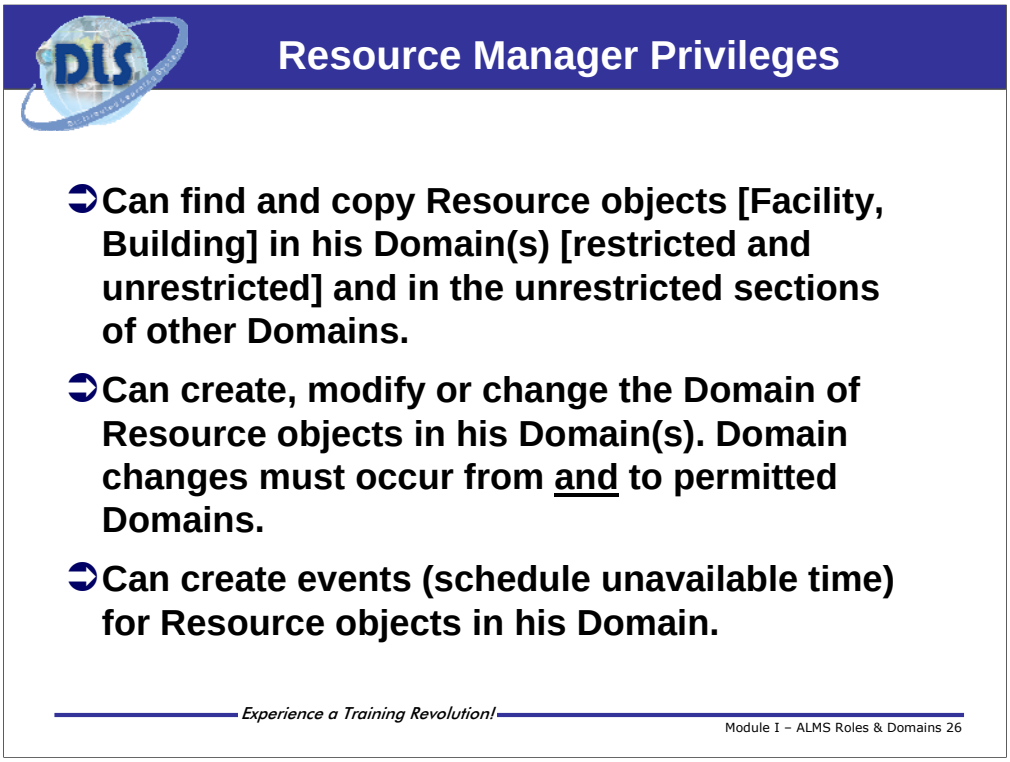
Courseware which is imported into the ALMS as a result of Process 4 will be placed in the Common Domain. Course Managers will normally move the Courseware into their own Domain for subsequent management. They can also copy database objects into their Domain from the Common Domain and from any other Unrestricted Domain. But to change the Domain from any domain other than own own and Common, the CoM needs to have privileges in the source Domain as well.



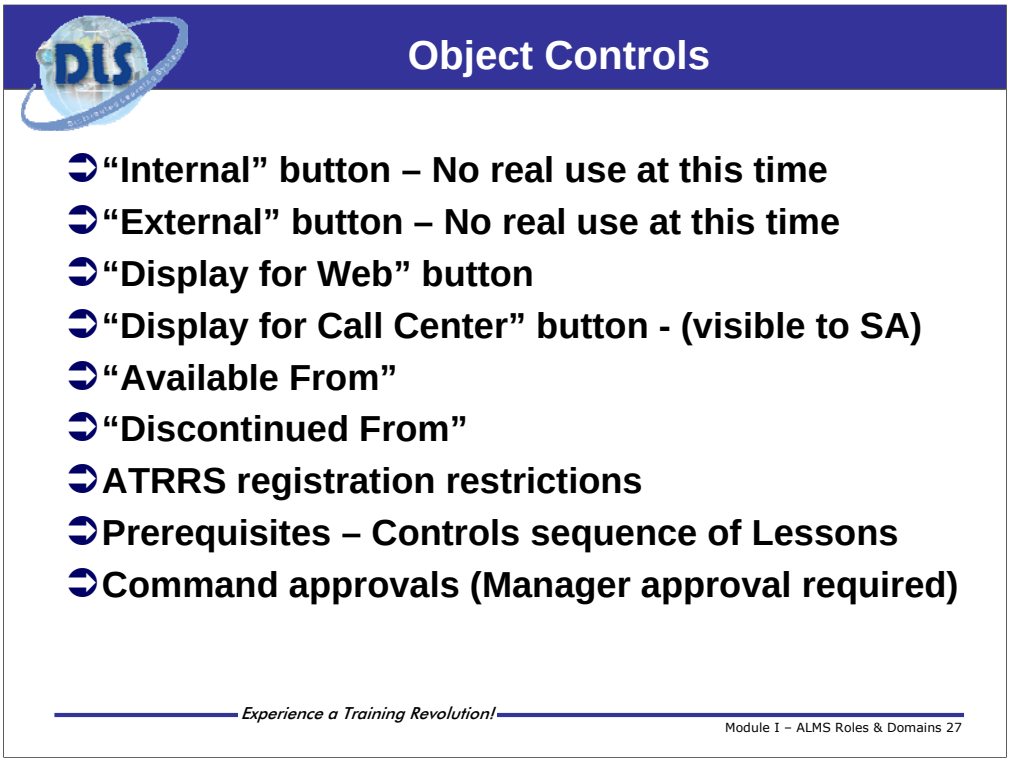
1st Bullet: These privileges closely parallel those of the CoM and Class Manager.

2nd Bullet: Note that Schedulers do not have Domain changing permissions.

3rd Bullet: The effect of the the third bullet is that a Resource such as a Facility for example can be "booked" by a Scheduler outside the Facility's Domain, if it is in the Unrestricted section of that Domain.



In short, what these rules mean is that Resources in the Unrestricted section of a Domain are available for scheduling by an ALMS Role Based User in another Domain. If the Resource is in the Restricted section of the Domain, it is schedulable only by Role-Based Users of that Domain with scheduling or event creating privileges.



In addition to Roles and Domains, the ALMS training access through other built-in features. These are:

Internal/External Check Boxes: While available, there is no real functional use for this feature at this time. Everything is internal.

Display for Web/Call Center Check Boxes: These boxes determine whether the item is visible for "the Web" (meaning can it be seen in the Catalog by a Learner), or for "Call Center" (meaning it is visible to System Administrators).

Available/Discontinued From: These dates, used primarily for training Products, control the window visibility of that Product inn the Catalog. It effectively defines the life span for that Product.

ATRRS Registration Restrictions: ATRRS has its own means of controlling access and the ability to register for Courses. The LMS always accepts database updates, such as Course registrations, from ATRRS, because they have passed the ATRRS gatekeepers.

Prerequisites: At the Course or stand-alone Product level, these determine whether a Learner can register for a Course. At the Lesson level, they control the sequence Lessons must be taken.

Command Approvals: This function just internalizes a process the Army has long has in place. There are some Courses which require the permission of someone in the Learner's chain of command before he is allowed to register for it. In the LMS, that individual has the Role of Training Approver.

Altogether Course and Class Managers have an extensive array of tools to control access to training. That means control who can register for and take what Courses under what conditions.

Summary

What We've Learned …

- Purpose of Roles and Domains
- How Roles and Domains are implemented in the ALMS
- Characteristics and types of Roles
- Characteristics and variety of Domains
- Other mechanisms for controlling access